CLAIMS

1. Method for security management in a node of a data processing network comprising a plurality of nodes, wherein each node maintains topology data representing the network, the method comprising:

evaluating an event received by the node from a neighboring node in the network to determine if the event satisfies a predetermined security test; and,

if the event fails the security test, modifying an entry associated with the neighboring node in the topology data maintained by the node, and sending an alarm notification indicative of the security failure to other nodes of the network.

2. Method as claimed in claim 1, wherein the sending step includes sending the alarm notification to all nodes of the network.

3. Method as claimed in claim 1, wherein the evaluating of the event received from the neighboring node comprises:

counting the number of occurrences of the event in a predetermined time interval;

incrementing a rating of the neighboring node if the number of occurrences exceeds a predetermined event occurrence threshold; and,

determining that the event fails the security test if the rating of the neighboring node exceeds a predetermined rating threshold.

4. Method as claimed in claim 1, comprising:

receiving an alarm notification generated by another node in the network, the received alarm notification being indicative of an event caused by a further node in the network;

evaluating the alarm notification received generated by the other node to determine if the other node satisfies a predetermined trust test, and,

evaluating the event indicated by the alarm notification if the other node passes the trust test to determine if the event indicated by the alarm notification satisfies the security test; and,

if the event fails the security test, modifying the topology data associated with the event causing node in the topology data maintained by the node, and sending another alarm notification indicative of the security failure to other nodes of the network.

5. Method as claimed in claim 4, wherein the evaluating of the event indicated by the alarm notification comprises:

counting the number of occurrences of the event indicated by the alarm notification in a predetermined time interval;

incrementing a rating of the event causing node if the number of occurrences exceeds a predetermined event occurrence threshold; and,

determining that the event fails the security test if the rating of the event causing node exceeds a predetermined rating threshold.

6. Computer program product comprising a computer readable medium having embodied therein computer readable program code means for causing a processor of a node in a data processing

network comprising a plurality of nodes to perform a method for security management in the node, wherein each node maintains topology data representing the network, the method comprising:

evaluating an event received by the node from a neighboring node in the network to determine if the event satisfies a predetermined security test; and,

if the event fails the security test, modifying an entry associated with the neighboring node in the topology data maintained by the node, and sending an alarm notification indicative of the security failure to any other nodes of the network.

7. Computer program product as claimed in claim 6, wherein the sending step includes sending the alarm notification to all nodes in the network.

8. Computer program product as claimed in claim 6, wherein the evaluating of the event received from the neighboring node comprises:

counting the number of occurrences of the event in a predetermined time interval;

incrementing a rating of the neighboring node if the number of occurrences exceeds a predetermined event occurrence threshold; and,

determining that the event fails the security test if the rating of the neighboring node exceeds a predetermined rating threshold.

9. Computer program product as claimed in claim 6, comprising:

receiving an alarm notification generated by another node in the network, the received alarm notification being indicative of an event caused by a further node in the network;

evaluating the alarm notification generated by the other node to determine if the other node satisfies a predetermined trust test, and,

evaluating the event indicated by the alarm notification if the other node passes the trust test to determine if the event indicated by the alarm notification satisfies the security test; and,

if the event indicated by the alarm notification fails the security test, modifying the topology data associated with the event causing node in the topology data maintained by the node, and sending another alarm notification indicative of the security failure to other nodes of the network.

10. Computer program product as claimed in claim 9, wherein the evaluating of the event indicated by the alarm notification comprises:

counting the number of occurrences of the event indicated by the alarm notification in a predetermined time interval;

incrementing a rating of the event causing node if the number of occurrences exceeds a predetermined event occurrence threshold; and,

determining that the event indicated by the alarm notification fails the security test if the rating of the event causing node exceeds a predetermined rating threshold.

11. Apparatus for security management in a node of a data processing network comprising a plurality of nodes, wherein each

node maintains topology data representing the network, the apparatus comprising control logic configured to evaluate an event received by the node from a neighboring node in the network to determine if the event satisfies a predetermined security test, to modify an entry associated with the neighboring node in the topology data maintained by the node if the event fails the security test, and to send an alarm notification indicative of the security failure to other nodes in the network.

12. Apparatus as claimed in claim 11, wherein the control logic is configured to send the alarm notification to all nodes of the network.

13. Apparatus as claimed in claim 11, wherein the control logic is configured such that evaluating the event received from the neighboring node comprises counting the number of occurrences of the event in a predetermined time interval, incrementing a rating of the neighboring node if the number of occurrences exceeds a predetermined event occurrence threshold, and, determining that the event fails the security test if the rating of the neighboring node exceeds a predetermined rating threshold.

14. Apparatus as claimed in claim 11, wherein the control logic is configured: to receive an alarm notification generated by another node in the network, the received alarm notification being indicative of an event caused by a further node in the network; to evaluate the received alarm notification to determine if the other node satisfies a predetermined trust test; to evaluate the event indicated by the alarm notification if the other node passes the trust test to determine if the event

indicated by the alarm notification satisfies the security test; to modify the topology data associated with the event causing node in the topology data maintained by the node if the event indicated by the alarm notification fails the security test; and, to send another alarm notification indicative of the security failure to other nodes of the network.

15. Apparatus as claimed in claim 14, wherein the control logic is configured such that evaluating of the event indicated by the alarm notification comprises: counting the number of occurrences of the event indicated by the alarm notification in a predetermined time interval; incrementing a rating of the event causing node if the number of occurrences exceeds a predetermined event occurrence threshold; and, determining that the event indicated by the alarm notification fails the security test if the rating of the event causing node exceeds a predetermined rating threshold.

16. Apparatus as claimed in claim 11, further comprising a memory for storing the topology data.

17. Data processing node for connection to a data processing network comprising a plurality of nodes, wherein each node maintains topology data representing the network, the data processing node comprising: a memory for storing the topology data; and, security management control logic connected to the memory and configured to evaluate an event received by the node from a neighboring node in the network to determine if the event satisfies a predetermined security test, to modify an entry associated with the neighboring node in the topology data stored

in the memory if the event fails the security test, and to send an alarm notification indicative of the security failure to other nodes of the network.

18. Data processing node as claimed in claim 17, wherein the control logic is configured to send the alarm notification to all neighboring nodes.

19. Data processing node as claimed in claim 17, wherein the control logic is configured such that evaluating the event received from the neighboring node comprises counting the number of occurrences of the event in a predetermined time interval, incrementing a rating of the neighboring node if the number of occurrences exceeds a predetermined event occurrence threshold, and, determining that the event fails the security test if the rating of the neighboring node exceeds a predetermined rating threshold.

20. Data processing node as claimed in claim 17, wherein the control logic is configured: to receive an alarm notification generated by another node in the network, the received alarm notification being indicative of an event caused by a further node in the network; to evaluate the received alarm notification to determine if the other node satisfies a predetermined trust test; to evaluate the event indicated by the alarm notification if the other node passes the trust test to determine if the event indicated by the alarm notification satisfies the security test; to modify the topology data associated with the event causing node in the topology data stored in the memory if the event indicated by the alarm notification fails the security test; and,

to send another alarm notification indicative of the security failure to other nodes of the network.

21. Data processing node as claimed in claim 20, wherein the control logic is configured such that evaluating of the event indicated by the alarm notification comprises: counting the number of occurrences of the event indicated by the alarm notification in a predetermined time interval; incrementing a rating of the event causing node if the number of occurrences exceeds a predetermined event occurrence threshold; and, determining that the event indicated by the alarm notification fails the security test if the rating of the event causing node exceeds a predetermined rating threshold.

22. Data processing network comprising a plurality of data processing nodes, wherein each node maintains topology data representing the network, each of the data processing nodes comprising: a memory for storing the topology data; and, security management control logic connected to the memory and configured to evaluate an event received by the node from a neighboring node in the network to determine if the event satisfies a predetermined security test, to modify an entry associated with the neighboring node in the topology data stored in the memory if the event fails the security test, and to send an alarm notification indicative of the security failure to any other nodes of the network.

23. Data processing network as claimed in claim 22, wherein the control logic is configured to send the alarm notification to all nodes of the network.

24. Data processing network as claimed in claim 22, wherein the control logic is configured such that evaluating the event received from the neighboring node comprises counting the number of occurrences of the event in a predetermined time interval, incrementing a rating of the neighboring node if the number of occurrences exceeds a predetermined event occurrence threshold, and, determining that the event fails the security test if the rating of the neighboring node exceeds a predetermined rating threshold.

25. Data processing network as claimed in claim 22, wherein the control logic is configured: to receive an alarm notification generated by another node in the network, the received alarm notification being indicative of an event caused by a further node in the network; to evaluate the received alarm notification to determine if the other node satisfies a predetermined trust test; to evaluate the event indicated by the alarm notification if the other node passes the trust test to determine if the event indicated by the alarm notification satisfies the security test; modifying the topology data associated with the event causing node in the topology data stored in the memory if the event indicated by the alarm notification fails the security test; and, to send another alarm notification indicative of the security failure to other nodes of the network.

26. Data processing node as claimed in claim 25, wherein the control logic is configured such that evaluating of the event indicated by the alarm notification comprises: counting the number of occurrences of the event indicated by the alarm

notification in a predetermined time interval; incrementing a rating of the event causing node if the number of occurrences exceeds a predetermined event occurrence threshold; and, determining that the event indicated by the alarm notification fails the security test if the rating of the event causing node exceeds a predetermined rating threshold.